RESOLUCIÓN NÚMERO 000181 DEL 27 ABR 2022

"Por la cual se actualizan los lineamientos del Sistema de Gestión de Seguridad de Información de la Entidad y la política de seguridad, privacidad de información y seguridad digital y se deroga la resolución 000683 del 17 de Diciembre de 2020"

**EL DIRECTOR GENERAL DE LA UNIDAD DE SERVICIOS PENITENCIARIOS Y CARCELARIOS - USPEC**

En uso de las facultades legales y en especial la conferida en el artículo 12 del Decreto 4150 de 2011, Decreto 1293 de 2020 y

**CONSIDERANDO**

Que, el artículo 12 del Decreto 4150 de 2011 faculta al Director General para implementar, mantener y mejorar el Sistema de Gestión Institucional de la Unidad de Servicios Penitenciarios y Carelarios – USPEC.

Que, la Ley 527 de 1999 define la firma digital como "Un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación"

Que, el artículo 2.2.2.47.1 del Decreto 1074 de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo", define la Firma electrónica como "Métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente."

Que, el CONPES 3854 de 2016 establece la Política Nacional de Seguridad Digital en la República de Colombia y busca fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socieconómicas en el entorno digital, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vz impulsará una mayor prosperidad económica del país.

Que, el Decreto 1499 de 2017, por el cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector de Función Pública, adopta la actualización del Modelo Integrado de Planeación y Gestión - MIPG, definiéndolo en su título 2, capítulo 1, artículo 2.2.22.3.2 como *"(...) un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio"*. Así mismo en su capítulo 2, artículo 2.2.22.2.1 se define *"Las Políticas de Gestión y Desempeño Institucional. Las políticas de Desarrollo Administrativo de que trata la Ley 489 de 1998, formuladas por el Departamento Administrativo de la Función Pública y los demás líderes, se denominan políticas de Gestión y Desempeño Institucional y comprenderán, entre otras, las siguientes(...) 12. Seguridad Digital"*.

Que, el capítulo I sección 2 artículo 2.2.9.1.1.3. del Decreto 1008 de 2018 incluye la seguridad de la Información entre los principios de la Política de Gobierno Digital, igualmente el artículo 2.2.9.1.2.1 define la seguridad de la información como habilitador transversal de la Política de Gobierno Digital que junto con los demás habilitadores permiten el desarrollo de los componentes y logros incluidos en dicha política.

Que, el parágrafo del articulo 16 del Decreto 2016 de 2019, establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones

Que el CONPES 3995 del 2020 establece la Política Nacional de Confianza y Seguridad Digital, a través de los cuales se pretende establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías.

"Por la cual se actualizan los lineamientos del Sistema de Gestión de Seguridad de Información de la Entidad y la política de seguridad, privacidad de información y seguridad digital y se deroga la resolución 000683 del 17 de Diciembre de 2020"

Que, a través de la Resolución 500 de 2021, emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, "se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital". Esta resolución tiene por objetivo establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI y la guía de gestión de riesgos de seguridad de la información y el procedimiento para la gestión de los incidentes de seguridad digital, . asi mismo, establece las directrices y estándares para la estrategia de seguridad digital. a los sujetos obligados señalados en el artículo 2.2.9.1.1.2 del Decreto 1078 de 2015.

El artículo 5 de la misma resolución establece que los sujetos obligados deben adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, formatos, manuales y lineamientos para la gestión de la seguridad de la información digital. Dicha estrategia se debe incluir en el Plan de Seguridad y Privacidad de Información que se integra al plan de acción en los términos del artículo 2.2.22.3.14 del capitulo 3 del Titulo 2 de la parte 2 del Libro 2 del Decreto 1083 del 2015, Unico reglamentario del Sector de Función Pública, o la norma que la modifique, adicione, subrogue o derogue. Así como adaptar el Modelo de Seguridad y Privacidad de Información – MSPI, señalado en el Anexo 1 de la misma resolución, como habilitador de la Política de Gobierno Digital.

Que, en la implementación del Sistema de Gestión de Seguridad de la Información(en adelante SGSI), es preciso establecer el alcance, la Política de Seguridad de la Información, los objetivos y los roles y responsabilidades de Seguridad de la Información, así como las políticas adicionales del Sistema de Gestión de conformidad con la norma NTC-ISO-IEC 27001:2013 a través del presente acto administrativo.

Que, a través de la Resolución 000683 de 2020 se actualizó la política de seguridad y privacidad de información de la Unidad de Servicios Penitenciarios y Carcelarios – USPEC, siendo necesario actualizar la política de seguridad y privacidad de información, modifcando roles y responsabilidades y las políticas específicas, e inlcuyendo el compromiso de la alta dirección y el seguimiento, medición, análisis y evaluación del SGSI.

Que en sesión del Comité Institucional de Gestión y Desemepeño de la Unidad de Servicios Penitenciarios y Carcelarios – USPEC, celebrada el 11 de febrero de 2022, se socializó a los miembros de este comité, la actualización efectuada al documento de la Política de Seguridad y Privacidad de Información de la Unidad de Servicios Penitenciarios y Carcelarios – USPEC, y en la misma sesión, se dio aprobación por parte del comité a esta política.

Que en virtud de lo anterior;

**RESUELVE:**

## CAPÍTULO 1
## GENERALIDADES DE LA POLÍTICA

**ARTÍCULO 1. Objeto:** La presente resolución tiene como objeto actualizar los lineamientos del Sistema de Gestión de Seguridad de información - SGSI y la Política de Seguridad, Privacidad de la Información y Seguridad Digital en la Unidad de Servicios Penitenciarios y Carcelarios – USPEC, así como actualizar los roles y responsabilidades y demás políticas propias frente a la implementación del SGSI.

**ARTÍCULO 2. Política General de Seguridad, Privacidad de la Información y Seguridad Digital.** Por la cual se actualiza la Política General de Seguridad, Privacidad de la Información y Seguridad Digital que se incorpora con la presente resolución y quedará así:

> "La UNIDAD DE SERVICIOS PENITENCIARIOS Y CARCELARIOS, a través de la implementación del Modelo de Seguridad y privacidad de Información – MSPI, enmarcado en el Sistema de Gestión de Seguridad de Información y consciente de la importancia que representan los activos de información para el cumplimiento de su misión institucional, se compromete a preservar la confidencialidad, integridad y disponibilidad de la información a través de la gestión de los

riesgos, la implementación estrategias y controles, el cumplimiento de los objetivos de seguridad de la información, los requisitos legales, organizacionales y obligaciones contractuales, y de la asignación de los recursos necesarios para mejorar continuamente el Sistema de Gestión de Seguridad de la Información".

**ARTÍCULO 3. Objetivos de Seguridad de la Información.** Para la implementación de la presente política se establecen los siguientes objetivos:

- Gestionar los riesgos de seguridad digital, con el fin de implementar controles que permitan proteger los activos de información que soportan la estrategia y operación de la Entidad.
- Capacitar y sensibilizar al personal de la USPEC en temas relacionados con seguridad de información, con el fin de fortalecer la toma de conciencia del personal de la Entidad.
- Gestionar los incidentes de seguridad de la información generando, documentando y aplicando las lecciones aprendidas, con el fin de reducir la probabilidad o el impacto de incidentes futuros.
- Implementar acciones preventivas, correctivas y de mejora generadas como resultado de las auditorias internas y/o externas con el fin de apoyar la mejora continúa del sistema de gestión de seguridad de información.

**ARTÍCULO 4. Alcance de la política.** La Política de Seguridad, Privacidad de la Información y seguridad digital aplica a todos los procesos institucionales, a todos los funcionarios, contratistas, proveedores, así como a todas aquellas personas o terceros que en razón del cumplimiento de sus funciones y las de la USPEC, compartan, utilicen, recolecten, procesen, intercambien o consulten su información, a los Entes de Control u otras Entidades relacionadas que accedan ya sea interna o externamiente a cualquier activo de información, independientemente de su ubicación. De igual manera, la presente política aplica a toda la información creada, procesada o utilizada, sin importantar el medio, formato, presentación o lugar en el que se encuentre. La implementación del SGSI en la USPEC se realizará acorde a los lineamientos contenidos en el Modelo de Seguridad y Privacidad de la Información y los requisitos de la Norma ISO 27001 en su versión vigente.

**ARTÍCULO 5. Compromiso de la Alta Dirección.** La Alta Dirección de la Unidad de Servicios Penitenciarios y Carcelarios – USPEC, se compromete a apoyar y liderar el establecimiento, implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información - SGSI; así mismo, se compromete a revisar el avance de la implementación del SGSI semestralmente y también garantizará los recursos suficientes (tecnológicos y talento humano calificado) para implementar y mantener el sistema, incluyendo las decisiones estratégicas de la seguridad de la información.

## CAPÍTULO 2
## ROLES Y RESPONSABILIDADES DE SEGURIDAD DE INFORMACIÓN

**ARTÍCULO 6.** A continuación se describen tanto los roles como las responsabilidades que se deben asumir al interior de la USPEC para la implementación y mejora continua del Sistema de Gestión de Seguridad de Información.

A. **Dirección General:** Responsable por el direccionamiento estratégico e impulso del Sistema de Gestión de Seguridad de Información. Establece su compromiso, mediante la asignación de recursos, responsabilidades y revisiones internas. Como parte de la gestión de la Dirección General para seguridad de la información se establecerán los lineamientos para:

1. La asignación de roles y responsabilidades de seguridad de la información.
2. La definición de la política general, objetivos, políticas específicas de seguridad de información y que estos sean compatibles con la planeación estratégica de la Entidad.
3. La asignación de los recursos necesarios para el mantenimiento del SGSI.

4. La revisión del Sistema de Gestión de Seguridad de la Información de la Entidad semestralmente, para asegurarse de su conveniencia, adecuación y eficacia continua. Esta revisión se realizará conforme a la información remitida por el Responsable de Seguridad de Información.
5. La dirección y apoyo a los funcionarios y/o contratistas para contribuir a la eficacia, mejora continua y logro de los resultados previstos dentro del SGSI.
6. El apoyo a otros roles pertinentes de la dirección, para demostrar su liderazgo dentro del SGSI aplicado a sus áreas de responsabilidad.

B. **Responsables de proceso:** Director, Jefe de Oficina o Líder encargado de proceso, quienes deberán asumir y ejecutar las siguientes responsabilidades:

1. Asignar los integrantes para la conformación del Equipo Operativo SGSI del(los) proceso(s) a cargo.
2. Difundir las políticas, procedimientos y demás documentos relacionados con el SGSI en su respectivo proceso.
3. Mantener actualizado el inventario de activos de información de su proceso de acuerdo a la metodología establecida por la entidad y propender por la ejecución de los controles requeridos para asegurar la confidencialidad, integridad y disponibilidad de los mismos.
4. Liderar la gestión para llevar a cabo la actualización de riesgos de seguridad digital al interior de su proceso según la metodología establecida por la Entidad.
5. Definir el plan de tratamiento de riesgos de seguridad digital, aprobarlo y velar por su cumplimiento.
6. Gestionar los recursos humanos, financieros, tecnológicos, materiales, necesarios para la mitigación de riesgos de seguridad digital a través de la implementación de controles definidos en los planes de tratamiento de riesgos.
7. Asegurar la disponibilidad de los Funcionarios y Contratistas de su proceso para la asistencia a actividades de formación y sensibilización que permitan el fortalecimiento de la cultura en Seguridad de la Información.
8. Gestionar la definición y ejecución de planes de mejoramiento requeridos para apoyar la mejora continua del SGSI.
9. Aprobar los planes, procedimientos y demás documentación necesaria para el mantenimiento del SGSI acorde a su proceso.
10. Las demás responsabilidades asignadas en los procedimientos, instructivos, guías y demás documentación del SGSI.

C. **Responsable de Seguridad de la Información:**

1. Liderar el mantenimiento del MSPI velando por el cumplimiento de las políticas de seguridad establecidas en la Entidad, los objetivos y planes del SGSI de forma que se encuentren alineados con los requerimientos de normas y leyes vigentes.
2. Realizar actualizaciones de las metodologías y políticas de Seguridad de la Información.
3. Socializar con funcionarios y contratistas de la Entidad los lineamientos del SGSI.
4. Acompañar a los procesos en la actualización de activos de información, riesgos de seguridad digital y la definición de los planes de tratamiento.
5. Realizar seguimiento a la ejecución de todos los planes que forman parte del SGSI.
6. Definir métodos que permitan identificar las vulnerabilidades en la infraestructura tecnológica de la Entidad.
7. Atender las auditorías internas, externas y revisiones de entes de control, proporcionando la información correspondiente a Seguridad de la Información.
8. Asegurar la adecuada gestión de los incidentes de seguridad de la información en la USPEC.
9. Definir las mediciones requeridas para verificar el desempeño del SGSI.
10. Mantener actualizada la declaración de aplicabilidad definiendo la justificación de las inclusiones de los controles implementados o justificación de aquellos que se pueden considerar como exclusión en el SGSI. Esta actualización se llevará a cabo de forma anual, posterior a la actualización del mapa de riesgos de seguridad digital con el fin de incluir los controles implementados en el tratamiento de riesgos.
11. Coordinar las actividades y reuniones del equipo operativo de seguridad de información.
12. Informar semestralmente a la Alta Dirección sobre el desempeño del sistema de gestión de seguridad de información a través del informe de revisión por la Dirección.
13. Revisar que el sistema se encuentre conforme con los requisitos de la Norma ISO 27001:2013 y el MSPI y mantener actualizada la herramienta de diagnóstico del MSPI.
14. Adelantar las gestiones pertinentes para llevar a cabo ejercicios de auditoria al SGSI.

15. Informar a las dependencias, cuando se detecten irregularidades, incidentes o prácticas que atenten contra la seguridad y privacidad de la información de acuerdo con la normativa vigente.

D. **Comité Institucional de Gestión y Desempeño.**
La conformación de este Comité se encuentra establecida en la Resolución 613 del 03 de diciembre de 2020, por la cual se adopta el Modelo Integrado de Planeación y Gestión Institucional – MIPG en la Unidad de Servicios Penitenciarios y Carcelarios – USPEC. Para el Sistema de Gestión de Seguridad de Información, se adoptarán las responsabilidades allí establecidas.

E. **Oficina Asesora Jurídica**

1. Orientar jurídicamente a los procesos institucionales de la Entidad, así como al Comité Institucional de Gestión y Desempeño en temas normativos, jurídicos y legales que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información.
2. Representar a la Entidad en procesos judiciales ante las autoridades competentes relacionados con seguridad y privacidad de la información.
3. Apoyar y asesorar a los procesos en la elaboración del Índice de Información clasificada y reservada de los activos de información de acuerdo con la regulación vigente

F. **Dirección de Gestión Contractual**

1. Verificar que los contratos que por competencia deban suscribir las dependencias de la Entidad, cuenten con cláusulas de derechos de autor, confidencialidad y no divulgación de la información según sea el caso.

G. **Grupo Administración de Personal**

1. Controlar y salvaguardar las historias laborales del personal de planta de la Entidad, en concordancia con la normatividad vigente.
2. Realizar la gestión de vinculación y desvinculación del personal de planta dando cumplimiento a los controles y normatividad vigente relacionada con seguridad y privacidad de la información.

H. **Oficina de Control Interno**

1. Incluir la seguridad de la información, dentro de los planes de auditoría institucionales.
2. Realizar seguimiento y evaluación de los controles establecidos para mitigar riesgos de seguridad de información.
3. Realizar seguimiento a los planes de mejoramiento de seguridad de información y determinar la efectividad de las acciones tomadas.

I. **Oficina de Tecnología**

1. Implementar los controles de tipo tecnológico que ayuden a mitigar los riesgos de seguridad de la información.

J. **Equipo Operativo de Seguridad de Información:** Este equipo está integrado por delegados de cada proceso institucional y dentro de sus responsabilidades se encuentran las siguientes:

1. Apoyar la actualización del inventario de activos de su proceso teniendo en cuenta la metodología definida por la Entidad.
2. Apoyar la actualización de riesgos de seguridad digital y la formulación de su respectivo plan de tratamiento de riesgos.
3. Apoyar a los responsables de la implementación del plan de tratamiento de riesgos de su proceso en la ejecución de controles según lo requerido.
4. Realizar seguimiento al interior de su proceso al plan de tratamiento de riesgos definido para mitigar los riesgos de seguridad digital y los demás planes relacionados con el cumplimento de lineamientos de seguridad de información.
5. Participar en las actividades de formación y sensibilización organizadas por el Sistema de Gestión de Seguridad de Información.
6. Apoyar la definición de los planes de mejoramiento requeridos para evidenciar la mejora continua del SGSI.

7. Difundir al interior de su proceso las políticas, procedimientos y demás documentos que hacen parte del SGSI.

El Equipo Operativo de Seguridad de la Información se reunirá de acuerdo con las necesidades del Sistema de Gestión de Seguridad de Información y por solicitud del Responsable de Seguridad de Información.

K. **Funcionarios y Contratistas:**

1. Apoyar el mantenimiento y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información, de acuerdo con las políticas, metodologías, procesos, procedimientos y los demás lineamientos establecidos para tal fin.
2. Aceptar y dar cumplimiento a las políticas y demás lineamientos de seguridad de la información
3. Ejecutar los controles que al interior de su proceso y la Entidad se requieran para la adecuada protección de los activos que se encuentran bajo su gestión.
4. Reportar eventos y/o incidentes de seguridad de la información de acuerdo al procedimiento establecido por la Entidad.
5. Clasificar, etiquetar y manejar la información de acuerdo con los procedimientos y políticas establecidas por la Entidad.
6. Participar activamente en las actividades de sensibilización, formación y toma de conciencia desarrolladas por la Entidad.

## CAPÍTULO 3
## POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE INFORMACIÓN

**ARTÍCULO 7. Política de seguridad de los recursos humanos.** El Grupo de Administración de Personal a cargo de la Dirección Administrativa y Financiera establecerá los lineamientos de seguridad que se deben cumplir durante los procesos de vinculación de personal, la ejecución del trabajo y en la terminación del vínculo laboral o cuando se presenten cambios de roles o funciones. Así mismo, el Grupo de Talento Humano será el responsable de llevar a cabo el proceso de inducción y reinducción en seguridad de información para el personal adscrito a la Entidad. Todo el personal que labore en la Entidad o preste servicios a la misma deberá firmar un acuerdo de confidencialidad de información.

**Parágrafo**: Con el mismo propósito, la Dirección de Gestión Contractual establecerá en las minutas de contrato los lineamientos de seguridad de información a través de las cláusulas y obligaciones contractuales las cuales serán divulgadas y verificadas para su cumplimiento por cada supervisor de contrato.

**ARTÍCULO 8. Política para dispositivos móviles.** El Grupo Administrativo a cargo de la Dirección Administrativa y Financiera y la Oficina de Tecnología establecen los lineamientos y buenas prácticas para proteger la información de la USPEC almacenada y /o gestionada a través de dispositivos móviles.

**ARTÍCULO 9. Política de gestión de activos**. La Oficina Asesora Jurídica, el Grupo de Gestión Documental y la Oficina de Tecnología mantendrán actualizados los lineamientos para la adecuada valoración, clasificación y gestión de activos de la USPEC a través del TIMA002 Manual de Clasificación de Activos, con el fin de suministrar la protección adecuada de activos de la Entidad de acuerdo con la legislación y estándares vigentes.

Toda información sea física o digital generada, almacenada o transformada por los funcionarios, contratistas o proveedores de la Entidad, utilizando los recursos dispuestos por la Entidad para tal fin o en desempeño de sus labores o servicio contratado, son activos de información propiedad de la USPEC.

En cuanto a los activos dispuestos por la Entidad, para el apoyo de las labores desempeñadas por los funcionarios, contratistas o proveedores, únicamente se permitirá su utilización para ejecución de tareas establecidas en el ámbito laboral de la USPEC.

**ARTÍCULO 10. Política de control de acceso.** A través de esta política se definen las responsabilidades de seguridad que los usuarios deben aplicar para minimizar riesgos de accesos no autorizados a servicios tecnológicos, sistemas de información o aplicaciones administradas tanto por la Oficina de Tecnología como por las demás dependencias responsables. En el caso de los servicios o sistemas de información externos a los cuales los funcionarios y contratistas deben acceder como cumplimiento de sus

funciones u obligaciones contractuales, se deberán tener en cuenta los lineamientos de la Entidad responsable, pero así mismo la dependencia de la USPEC a cargo de su registro deberá mantener un registro de usuarios habilitados y deshabilitados del mismo y asegurar las gestiones correspondientes para la actualización de usuarios cuando haya lugar.

Todos los usuarios deben asumir la responsabilidad sobre la información física o digital que accedan y procesan dando un uso adecuado con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información.

**ARTÍCULO 11. Política de seguridad física y del entorno.** El Grupo Administrativo en cabeza de la Dirección Administrativa y Financiera debe establecer junto con las áreas responsables los lineamientos y controles de acceso físico para acceder a las zonas seguras de la Entidad, así como a las demás instalaciones de la USPEC, con el fin de permitir el acceso únicamente a personal autorizado. Adicionalmente se debe asignar la protección contra amenazas externas y ambientales, ubicación y protección de los equipos, retiro de los activos de las instalaciones y de la seguridad de los mismos fuera de las instalaciones.

**Parágrafo**: Todos los funcionarios, contratistas y visitantes que se encuentren en las instalaciones de la USPEC deben estar debidamente identificados a través del carné asignado por la Entidad y portarlo siempre en un lugar visible. En el caso de los funcionarios y contratistas deben emplear la tarjeta de acceso para ingresar y salir del edificio. Estos documentos de identificación son de carácter personal e intransferible.

**ARTÍCULO 12. Política sobre el uso de controles criptográficos.** La Oficina de Tecnología establecerá las herramientas a través de las cuales se puede llevar a cabo la encriptación de información institucional de carácter reservado o clasificado con el fin de mantener sus criterios de confidencialidad e integridad, previamente establecidos por la dependencia responsable de la información al momento de realizar transferencias de la misma.

**Parágrafo**: Las dependencias que requieran transferir información reservada o confidencialidad deberán informar a la Oficina de Tecnología con el fin de brindar orientación frente al proceso de encriptación.

**ARTÍCULO 13. Política teletrabajo o trabajo remoto.** Esta política define las condiciones, directrices, acuerdos y restricciones que deben implementarse en las diferentes modalidades de teletrabajo de la USPEC y el uso seguro de las herramientas tecnológicas suministradas para cumplir este propósito, las cuales se encuentran alineadas con la legislación colombiana vigente.

**ARTÍCULO 14. Política de escritorio y pantalla limpios.** Esta política establece los lineamientos para prevenir el acceso no autorizado, pérdida y/o daño de la información institucional, que se encuentra a cargo del personal que labora en la USPEC, almacenada en los puestos de trabajo, equipos de cómputo, medios extraíbles, dispositivos de impresión y digitalización de documentos, durante y fuera del horario laboral. Los documentos catalogados como reservados y/o clasificados no deberán permanecer en el escritorio físico, ni en el escritorio virtual. Se deberán emplear los espacios dispuestos por la Entidad para el almacenamiento de esta información.

**ARTÍCULO 15. Política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.** Para el manejo de llaves criptográficas (token) en la Entidad, se deben aplicar las siguientes medidas:

1. El uso de estos dispositivos está asociado a nombre propio de cada usuario, por lo tanto, no deben ser usados por personal ajeno, con el fin de contribuir con la integridad de la información.
2. Las contraseñas o passwords que se usen como mecanismo de identificación adicional al token deben cumplir con los requisitos de contraseñas seguras establecidos por la Oficina de Tecnología.
3. Las contraseñas o passwords utilizadas con estos dispositivos no se deben compartir y se debe garantizar que estas no sean conocidas por otras personas o sean divulgadas.
4. Cuando estos dispositivos se averíen y/o deban ser reemplazados, se debe garantizar la destrucción segura de los antiguos dispositivos, con el fin de evitar que puedan ser usados de manera ilegal o fraudulenta.
5. Siempre guardar estos dispositivos en lugares seguros, resguardados y en lo posible monitoreados, para evitar que sean accedidos y/o usados sin autorización, incluso cuando no se encuentren en uso.
6. En caso de pérdida o robo, o uso no autorizado debe ser reportado como un evento de seguridad de información a través de los canales establecidos para tal fin por la Oficina de Tecnología. Lo anterior con el fin de gestionar la revocación de los certificados o llaves privadas de cifrado y así evitar que se vulneren los accesos, la información o datos sensibles que se puedan gestionar con estos dispositivos.

7. Las llaves de cifrado deben ser renovadas como mínimo 1 vez al año o en lo posible, se deben realizar acuerdos con los proveedores para que éstas sean actualizadas cada 6 meses.
8. Es indispensable que se usen siempre desde equipos propios de la USPEC, con el fin de asegurar que no sean vulnerados en equipos con malware o que se encuentren en riesgo de ser infectado con tales amenazas.

**ARTÍCULO 16. Política de copias de respaldo.** La Oficina de Tecnología define los lineamientos y directrices que deben seguirse al interior de la Entidad para la realización de respaldo de la información del correo institucional y el backup de la Entidad, para asegurar que pueda efectuarse una recuperación adecuada en el momento que se requiera. Adicionalmente el Grupo de Gestión Documental definirá en conjunto con las dependencias, los tiempos de retención de la información a cargo de cada una de ellas con el propósito de establecer los tiempos de conservación.

**ARTÍCULO 17. Política de transferencia de información.** La Oficina de Tecnología establece los lineamientos para la transferencia de información institucional catalogada como reservada o clasificada. Los responsables del proceso son los encargados de autorizar las transferencias de la información sensible que tienen a su cargo y el receptor de la información es el responsable de aplicar los controles pertinentes de seguridad de información con el fin de mantener la confidencialidad e integridad de la misma.

**ARTÍCULO 18. Política de desarrollo seguro.** La Oficina de Tecnología establece los requerimientos de seguridad que se deben tener en cuenta durante el ciclo de vida del software, independientemente que se genere un proceso de adquisición, desarrollo o mantenimiento de un sistema de información. Así mismo el Responsable de Seguridad ejecutará pruebas de seguridad de información con el fin de validar si el sistema de información cumple con los parámetros establecidos para asegurar la confidencialidad, integridad y disponibilidad de la información.

Todos las dependencias de la Entidad deberán informar a la Oficina de Tecnología sobre sus proyectos de adquisición de sistemas de información, con el fin de brindar las observaciones correspondientes y revisar los aspectos técnicos necesario para su desarrollo e implementación.

Cualquier software que opere en la Unidad de Servicios Penitenciarios y Carcelarios deberá reportarse y entregarse a la Oficina de Tecnología cumpliendo con los lineamientos técnicos y estándar de desarrollo de software establecidos por la OTEC, con el fin de salvaguardar la información, brindar el soporte y demás procesos técnicos que permitan su recuperación en caso de algún incidente de seguridad de información.

**ARTÍCULO 19. Política de seguridad de la información para las relaciones con proveedores.** La Dirección de Gestión Contractual establece a través de las minutas de contrato los lineamientos de seguridad de la información que deben implementarse con los terceros que cuenten con privilegios para acceder, procesar y almacenar información de la USPEC. Es responsabilidad del supervisor de contrato divulgar las políticas y demás lineamientos de seguridad de información a los proveedores que tiene a su cargo.

La dependencia que requiere llevar a cabo un proceso de contratación, deberá establecer previamente los riesgos de seguridad de información y los controles para su mitigación. Una vez se inicie la ejecución del contrato deberá realizar seguimiento a la ejecución de los controles, con el fin de mitigar la materialización de los riesgos.

**ARTÍCULO 20. Política de Gestión de Incidentes.** La Oficina de Tecnología establecerá los lineamientos para la gestión de los incidentes de seguridad de información en la Entidad, así mismo se encargará de asignar el personal responsable para su tratamiento, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados. Todo el personal de la USPEC podrá reportar incidentes de seguridad a través de los canales establecidos para tal fin.

**ARTÍCULO 21.** Todas las políticas identificadas en este capítulo se deberán reglamentar de manera detallada en la declaración de aplicabilidad y la documentación propia del Sistema de Gestión de Seguridad de Información.

## CAPÍTULO 4
## REVISIÓN, VIGENCIA Y DEROGATORIA

"Por la cual se actualizan los lineamientos del Sistema de Gestión de Seguridad de Información de la Entidad y la política de seguridad, privacidad de información y seguridad digital y se deroga la resolución 000683 del 17 de Diciembre de 2020"

**ARTÍCULO 22. Actualización del alcance, política, objetivos, roles y responsabilidades de seguridad de la información.** La Política de Seguridad, Privacidad de la Información y seguridad digital se revisará anualmente, o antes si se presentan situaciones que puedan llegar a afectar la seguridad de la información en la Entidad. Esta gestión está a cargo del Responsable de Seguridad de Información o quien haga sus veces y será aprobada por el Director General de la USPEC.

**ARTÍCULO 23. Seguimiento, medición, análisis y evaluación del SGSI.** La USPEC realizará revisiones semestrales para determinar la conveniencia, adecuación y eficacia de la implementación del MSPI, a través del informe de revisión por la dirección, incluyendo los lineamientos establecidos en la Norma ISO 27001:2013. Esta información deberá ser revisada por el Comité Institucional de Gestión y Desempeño y como producto se deberán establecer los compromisos para la mejora del SGSI.

**ARTÍCULO 24. Incumplimiento de las políticas y lineamientos de seguridad de información.** El incumplimiento de las políticas mencionadas en la presente resolución, así como la violación de los procedimientos o lineamientos establecidos en temas de seguridad de información y de las leyes, decretos y demás normas que soporten estas políticas, se establecerá como un incidente de seguridad de información y se gestionará de acuerdo con los lineamientos establecidos por la Oficina de Tecnología. Adicionalmente conllevará en el caso de funcionarios, a la notificación de la situación que se evidencia a su jefe inmediato y en caso requerido se procederá a iniciar el proceso disciplinario teniendo en cuenta lo establecido en el procedimiento JUPRO2 Procesos disciplinarios de la Entidad, a cargo de la Oficina Asesora Jurídica.

En el caso de contratistas se enviará notificación al interventor y/o supervisor del contrato y copia a la Dirección de Gestión Contractual para que de acuerdo con sus competencias se generen las investigaciones a que haya lugar. En el caso de terceros, esto conlleva una nota solicitando explicación al representante legal de la firma a la que pertenece el contratista y en caso de manipulación indebida podrá tener efectos penales, de igual manera se notificará a los interventores y/o supervisores de contrato.

**ARTÍCULO 25.** La presente Resolución rige a partir de la fecha de su expedición, y deroga la Resolución 000683 del 17 de diciembre de 2020, así como todas aquellas disposiciones que le sean contrarias.

**PUBLÍQUESE Y CÚMPLASE**

Dada en Bogotá, D.C. a los 27 ABR 2022

**ANDRÉS ERNESTO DÍAZ HERNÁNDEZ**
Director General de la Unidad de Servicios Penitenciarios y Carcelarios - USPEC

Elaboró: Mayra Alexandra Agudelo Carvajal - Profesional Especializado

Revisó: Imelda Muñoz Mancipe - Jefe Oficina de Tecnología

Control de Legalidad: Fabio Rodriguez Días - Coordinador Grupo de acciones constitucionales, conceptos y control de legalidad
Ruta: No aplica.
Ubicación archivo físico: Carpeta seguridad de información